IN THE UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF OHIO EASTERN DIVISION

| UNITED STATES OF AMERICA, |) |
|---------------------------|--------------------------|
| D1 : |) Case No. 1:20-cr-0068 |
| Plaintiff, |) Judge Dan Aaron Polst |
| V. |) Judge Buil Haron Folse |
| | ORDER ORDER |
| DAVID JOHNSON, |) |
| Defendant. |) |
| | |

Before the Court is the government's unopposed motion *in limine* to authenticate phone call records and tower location data, email account data and geographical coordinates, and social media account records. The government's four exhibits (Exhibits A-D) contain certifications by records custodians that satisfy the authentication requirements under Fed. R. Evid. 803(6)(A)-(C), 902(11), and 902(13). Therefore, the Court <u>GRANTS</u> the government's motion to authenticate the following items:

- (a) T-Mobile call records and cellular tower location data for phone number (216) 394-7088;
- (b) Google/Gmail account data and geographical coordinates for email addresses KevinJefferies82@gmail.com, ChrisWilliamsR1985@gmail.com, also referred to as account 12163947088; and
- (c) Instagram Account 5756967395, 1chaseda_problemchild.

The Court's ruling that the above records are authentic does not limit the defendant's right at trial to oppose or challenge the admissibility of the records on other grounds.

Background

On October 22, 2020, a federal grand jury, in the Northern District of Ohio, returned a 9count indictment against the defendant, David Johnson, for a series of robberies and firearm offenses that occurred during November 2019 and January 2020. Counts 1, 3, 5, and 7 allege Interference with Commerce by Robbery, in violation of 18 U.S.C. § 1951(a). Counts 2, 4, 6, and 8, allege Use, Carry, and Brandishing a Firearm During and in Relation to a Crime of Violence, in violation of 18 U.S.C. § 924(c)(1)(A)(ii). And Count 9 alleges Felon in Possession of a Firearm, in violation of 18 U.S.C. § 922(g)(1) and 924(a)(2).

Procedural History

On November 21, 2022, in email correspondence with the parties, the Court ordered the government to file a motion regarding the authenticity of the records by December 2, 2022. The Court directed the defendant's reply by December 9, 2022. On December 1, 2022, the government filed its motion *in limine*. ECF Doc. 30. The defendant did not file a written reply and has not otherwise opposed the government's motion.

The government moves to authenticate the below records to streamline the presentation of evidence and avoid calling T-Mobile, Google, and Instagram/Facebook¹ representatives to solely authenticate these records:

- (a) T-Mobile call records and cellular tower location data for phone number (216) 394-7088;
- (b) Google/Gmail account data and geographical coordinates for email addresses KevinJefferies82@gmail.com, ChrisWilliamsR1985@gmail.com, also referred to as account 12163947088; and
- (c) Instagram Account 5756967395, 1chaseda_problemchild. *Id.* at p. 2.

¹ The government's motion refers to Instagram and Facebook interchangeably. ECF Doc. 30, pp. 1, 3, 5, 11. The government submitted a Certificate of Authenticity by a Facebook records custodian to authenticate Instagram account records. ECF Doc. 30-4 (Ex. D). The government appears to address this matter in a parenthetical that says, "both owned by Facebook." ECF Doc. 30, p. 1. The Court believes this discrepancy is attributed to the fact that in April 2012, Facebook Inc. bought Instagram and likely consolidated Instagram records requests under Facebook. The defendant has not objected to this issue or opposed the government's motion.

<u>Analysis</u>

The government argues that the above records are business records under Fed. R. Evid. 803(6) and, as such, they are self-authenticating under Fed. R. Evid. 902 (11). ECF Doc. 30, pp. 4-5. Additionally, the government moves to authenticate the phone provider records under Fed. R. Evid. 902(13). *Id.* at p. 7.

Fed. R. Evid. 901 and 902 govern the authentication of evidence. Fed. R. Evid. 901(a) requires a proponent of evidence to produce proof "sufficient to support a finding that the item is what the proponent claims it is." Fed. R. Evid. 902 provides a list of items that are "self-authenticating" and "require no extrinsic evidence of authenticity in order to be admitted." Under Fed. R. Evid. 902(11), certified domestic records of a regularly conducted activity that satisfy Fed. R. Evid. 803(6)(A)-(C) are self-authenticating. The relevant portion of Fed. R. Evid. 803(6) requires:

- (A) the record was made at or near the time by—or from information transmitted by—someone with knowledge;
- (B) the record was kept in the course of a regularly conducted activity of a business, organization, occupation, or calling, whether or not for profit; [and]
- (C) making the record was a regular practice of that activity[.]

Fed. R. Evid. 803(6)(A)-(C). Finally, Fed. R. Evid. 902(13) requires the records to be certified "as shown by a certification of a qualified person that complies with the certification requirements of Rule 902(11) or (12)."

The government satisfied the authentication requirements under Fed. R. Evid. 803(6)(A)-(C), 902(11), and 902(13) for the T-Mobile call records and tower location data, the Google/Gmail account data and geographical coordinates, and the Instagram account information.

First, regarding the T-Mobile call records and tower location data, the government provided a written declaration by a T-Mobile records custodian, dated February 12, 2020. ECF Doc. 30-1 (Ex. A). The custodian attested that the phone records were "made at or near the time of the occurrence," "by a person with knowledge of those matters," and were "kept in the course of regularly conducted business activity," which was "a regular practice" of T-Mobile. *Id.*Second, regarding the Google/Gmail account data and geographical coordinates, the government provided two affidavits by Google records custodians, dated February 28, 2020, and March 11, 2020. ECF Doc. 30-2, p. 4 (Ex. B); ECF Doc. 30-3, p. 3 (Ex. C). Both documents contain the following identical language that satisfies the authentication requirements under Fed. R. Evid. 803(6)(A)-(C), 902(11), and 902(13):

- 5. The Document is a record made and retained by Google. Google servers record this data automatically at the time, or reasonably soon after, it is entered or transmitted by the user, and this data is kept in the course of this regularly conducted activity and was made by regularly conducted activity as a regular practice of Google.
- 6. The Document is a true duplicate of original records that were generated by Google's electronic process or system that produces an accurate result. The accuracy of Google's electronic process and system is regularly verified by Google.

ECF Doc. 30-2, p. 4 (Ex. B); ECF Doc. 30-3, p. 3 (Ex. C).

Third, regarding the Instagram account, the government provided an affidavit from a Facebook records custodian, dated February 15, 2020. ECF Doc. 30-4 (Ex. D). In accordance with the authentication requirements under Fed. R. Evid. 803(6)(A)-(C), 902(11), and 902(13) the custodian certified that:

The records provided are an exact copy of the records that were made and kept by the automated systems of Facebook in the course of regularly conducted activity as a regular practice of Facebook. The records were saved in electronic format after searching Facebook's automated systems in accordance with the abovespecified legal process. The records were made at or near the time the information was transmitted by the Facebook user.

ECF Doc. 30-4 (Ex. D).

It is undisputed that the Government secured the requisite certifications to qualify the above records as self-authenticating business records. Additionally, there is no evidence to suggest a lack of trustworthiness or reliability in the government's records. Therefore, the government satisfied its burden in authenticating the T-Mobile call records and cellular tower location data, the Google/Gmail account data and geographical coordinates, and the Instagram account records. Using certificates of authenticity to authenticate these records at trial does not violate the Confrontation Clause. *See Melendez-Diaz v. Massachusetts*, 557 U.S. 305, 322, 129 S. Ct. 2527, 2539 (2009) (discussing the "general rule" that a "clerk's certificate authenticating an official record" was "traditionally admissible" at trial because of its non-testimonial nature); *see also United States v. Collins*, 799 F.3d 554, 585 (6th Cir. 2015) (finding no Confrontation Clause violation where the district court admitted the defendants' pharmacy records without inperson witness testimony to the individual transactions because the records were non-testimonial and "not made to prove the guilt or innocence of any particular individual, nor were they created for solely evidentiary purposes").

Conclusion

For the foregoing reasons, the Court <u>GRANTS</u> the government's unopposed motion *in limine* to authenticate the T-Mobile call records and cellular tower location data, the Google/Gmail account data and geographical coordinates, and the Instagram account records.

The Court finds that using certificates of authenticity for these records at trial does not violate the Confrontation Clause. The Court's ruling does not prevent the defendant from opposing the

Case: 1:20-cr-00682-DAP Doc #: 32 Filed: 12/16/22 6 of 6. PageID #: 255

admission of these records at trial. The defendant may still challenge their admissibility on other grounds.

IT IS SO ORDERED.

Date: December 16, 2022

/s/ Dan Aaron Polster
Dan Aaron Polster
United States District Judge